UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE USE OF A CELL-SITE SIMULATOR TO LOCATE THE CELLULAR DEVICE ASSIGNED CALL NUMBER 269-358-0496	Case No. 20-MJ- 226-01-AJ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Emily Munchiando, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 to authorize law enforcement to employ electronic investigative techniques, as described in the following attachment, to determine the location of the target cellular device assigned dialed number 269-358-0496**,** referred to in this affidavit as the "Target Cellular Device." The service provider for the target cellular device is AT&T. This affidavit is made in support of up to two different search warrants to locate the phone: 1) by obtaining information from the service provider, e.g., cell site information and/or 2) by utilizing a device that acts as a cell phone tower sometimes referred to as a

Cell Site Simulator, or a Wi-Fi geolocation device. In addition, because this request may be construed as a Pen Register / Trap and Trace device or request, the application for this warrant (which includes this affidavit) is intended to comply with 18 U.S.C. § 3122.

2. I am a Special Agent, with the Federal Bureau of Investigation. I have been so employed since approximately September of 2014. I am currently assigned to the Violent Crime Task Force (VCTF). As part of my duties, I investigate criminal violations concerning crimes of violence including federal violations of Title 18 and Title 21. I have experience in the investigation, apprehension and prosecution of individuals involved in federal criminal offenses, the use of cellular devices to commit those offenses and the available technology that can be used by law enforcement to assist in identifying the users of cellular devices and their location.

3. The facts in this affidavit come from my personal observations, training, experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of the information, known to law enforcement, related to this investigation.

4. There is reason to believe the target cellular device is currently located in this district. On December 11, 2020, the court authorized a search warrant to Ping the target cellular device. Ping data received from December 14, 2020 and December 15, 2020, indicated that the target cellular device is located in this district. However, due to the lack of precision associated with the pings, Agents have not been able to physically locate the target cellular device. Therefore, Agents seek the enclosed search warrant.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that Katelyn JONES, the daughter of Linda Jones, is using the Target Cellular Device. I know from training and experience that cell phone users normally have their cell telephones with them, so locating a user's cell phone will show that user's location. I believe that locating the Target Cellular Device will constitute and lead to evidence of violations of 18 U.S.C. § 875(c), Transmitting Threatening Communications in Interstate Commerce. I submit that there is also probable cause to believe that the location information described in Attachment B will constitute evidence of these criminal violations and will lead to the identification of an individual who is engaged in the commission of this offense.

PROBABLE CAUSE

6. Adult Victim 1 (AV-1) is the Chair of the Wayne County Board of Canvassers. Wayne County is the largest county in Michigan. As a member of the Board of Canvassers, AV-1 must vote for or against the certification of election results for Wayne County, Eastern District of Michigan.

7. On November 17, 2020, AV-1 voted against certifying the recent election results. AV-1's vote was reported on numerous news outlets, both locally and nationally.

8. On November 18, 2020, at approximately 7:46 a.m., AV-1 received multiple threatening text messages from an unknown person. The text messages were sent to AV-1's cellular phone and came from phone number (269) 319-8068. The text messages stated the following:

a. "Damn it was not hard finding all of your information disgusting racist bitch [AV-1's name], [AV-1's address];" and

b. "I don't tolerate people like you, in fact I consider you to be a terrorist and do you know what happens to terrorist [AV-1's first name]???"

9. The messages were immediately followed by two graphic photographs of a bloody deceased, nude, mutilated women lying on the ground. Immediately thereafter, a photograph of AV-1's daughter, who is a minor, was sent to AV-1.

10. Following the pictures, the individual sent additional text messages which stated the following:

a. "I'd just like you to imagine that's little [AV-1's daughter's name] your beautiful daughter." The "that's" reference was to the images of the bloody deceased, nude, mutilated women;

b. "Have you ever heard of a private opinion on your Facebook???" "I guess not;"

c. "Fucking with our election is TERRORISM, and us Americans clearly don't tolerate terrorist so yes you should be afraid, your daughter should be afraid and so should [name of AV-1's husband];"

d. "Tsk, Tsk, Tsk;" and

e. "You have made a grave mistake [AV-1's first name] I hope you realize that now."

11. Also on November 18, 2020, AV-1 received similar threats on AV-1's Instagram page by Instagram username, "_etfere" that were very similar to the threats made by telephone number (269) 319-8068. Instagram user, "_etfere" made

comments under numerous photographs on AV-1's Instagram page including, but not limited to, the following posts:

a. "[AV-1 phone number AV-1 address];"

b. "[AV-1's phone number] [AV-1's husband's phone number] [AV-1 address] Feel free to leave these disgusting racist a nice little message on their voicemail or for more fun stop by their house;"

c. "Racist Terrorist Bitch;"

d. "Idk [I don't know] if god would like you praying for a terrorist unless you're one too???"

e. "@dfit1coach we want her in more pain." The reference to "her" is AV-1;

f. "Your Daughter is beautiful," referring to AV-1's daughter;

g. "I'd be a shame if something happened to her." This comment was posted under a picture of AV-1, AV-1's daughter, and AV- 1's husband; and

h. "Hmmm I'd be a shame if something happened to your daughter at school."

12. Based on the similarities between the threatening text messages and threatening Instagram posts, I believe they were sent by the same individual. Both

the text and Instagram threatening messages were sent on the same day. They both use AV-1's name and AV-1's address. They both refer to AV-1 as a racist, bitch, and terrorist. Both sets of messages identify AV-1's husband and daughter. As to the daughter, both refer to her as "beautiful." Both threaten harm to AV-1's daughter. They both incorporate an image of AV-1's daughter in the threats. The threatening text messages include the image of the bloody and mutilated woman and states that AV-1's daughter "should be afraid." The Instagram threats state "shame if something happened to her," and "shame if something happened to your daughter at school."

13. On November 18, 2020, the Federal Bureau of Investigation National Threat Operations Center received a call from AV-1. AV-1 reported the threats made to AV-1 and AV-1's family through text messages and Instagram. AV-1 did not know the individual who sent the threatening texts or made the threatening comments on Instagram.

14. Instagram records associated with Instagram username "_etfere" resolved to the Instagram account, "i_dont_fukkin_play6925". The user of the "i_dont_fukkin_play6925" account provided the Target Cellular Device number to Instagram to register the account and for contact information. The Target Cellular Device was used to verify the account holder. When establishing an account, Instagram sends a confirmation text message to the registered phone, in this case

the Target Cellular Device, to finalize and verify the registration of the account. This verifies that an individual used the Target Cellular Device to create the "i_dont_fukkin_play6925" account.

15. On November 25, 2020, AV-1's local police department executed a search warrant on Instagram account, "i_dont_fukkin_play6925". The Instagram search warrant results revealed numerous photographs of a female. Based on how many images of the female were on the account, and the information in the account, I believe that the female was the user of this account. The female was subsequently identified as Katelyn JONES. The images from the Instagram account matched JONES's Michigan driver license photograph. The address on JONES's driver's license is in Olivet, Michigan.

16. Law enforcement databases indicated that the number that sent the threatening text messages, (269) 319-8068, was serviced by Onvoy Spectrum. Records provided by Onvoy LLC, d/b/a Inteliquent, showed that (269) 319-8068 was assigned to the service provider, TextMe Inc.

17. Records provided by TextMe Inc., for telephone number (269) 319-8068, identified an account created on November 18, 2020 at 7:36 a.m. (10 minutes before AV-1 received the threatening text messages) utilizing IP address, 2601:188:c300:e840:c1a:2af6:fdad:c844 (the IP address). This is the same day the threatening text messages and the threating Instagram posts were made.

18. An internet search of the IP address resolved to Comcast Cable Communications. Records provided by Comcast Cable Communications established that the subscriber to the IP Address was Linda K. Jones, 177 Main Street, Apt 4, Epping, New Hampshire, 03042. Linda K. Jones is 54 years-old. Katelyn JONES, the user of "i_dont_fukkin_play6925," is 23 years-old. Law enforcement databases suggest that they are related. Based on my training and experience, I believe Linda Jones is Katelyn JONES's mother.

19. Based on the information received from TextMe, Inc., on November 18, 2020, a TextMe account was created with the number 269-319-8068, with a device connected to Linda Jones's Comcast IP address, and used, 10 minutes later, to send the threatening text messages to AV-1.

20. The Target Cell Device and the number used to send the threatening text messages have the same 269 area code. Olivet, Michigan, Katelyn JONES'S registered address with the Michigan Secretary of State, is in the 269 area code. Further, the Target Cell Phone is registered to Katelyn JONES's registered address, 23090 T Drive North, Olivet, Michigan, 49076.

21. Based on my training and experience, probable cause exists that the Target Cellular Device belongs to or is used by Katelyn JONES. The Target Cellular Device was an instrumentality used to violate 18 U.S.C. § 875(c), Transmitting Threatening Communications in Interstate Commerce. Thus, tracking

the Target Cell Phone will assist law enforcement with locating both evidence of the crime contained on the Target Cellular Device and Katelyn JONES.

22. Information obtained from this search warrant will be used to attempt to locate Katelyn JONES, the daughter of Linda Jones, and the Target Cellular Device, within the next 30 days.

AUTHORIZATION REQUEST & MANNER OF EXECUTION

23. I request that the Court issue the proposed search warrant pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c).

24. Because collecting the information authorized by this warrant may fall within the statutory definitions of a "pen register" or a "trap and trace device," *see* 18 U.S.C. § 3127(3) & (4), this application and the accompanying warrant are intended to comply with requirements set forth in 18 U.S.C. §§ 3122-3123.

25. In my training and experience, I have learned that cellular phones and other cellular devices communicate wirelessly across a network of cellular infrastructure, including towers that route and connect individual communications. When sending or receiving a communication, a cellular device broadcasts certain signals to the cellular tower that is routing its communication. These signals include a cellular device's unique identifiers.

26. In my training and experience, I have learned that AT&T is a company with its headquarters located within the United States and provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate at least two kinds of information about the locations of the cellular telephones to which they provide service: (1) E-911 Phase II data, also known as GPS data or latitude-longitude data, and (2) cell-site data, also known as "tower/face information" or cell tower/sector records. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device.

27. To facilitate execution of this warrant, law enforcement may use an investigative device or devices (sometimes referred to as a Cell Site Simulator or

Wi-Fi geolocation device) capable of broadcasting signals that will be received by the Target Cellular Device or receiving signals from nearby cellular devices, including the Target Cellular Device. Such a device may function in some respects like a cellular tower, except that it will not be connected to the cellular network and cannot be used by a cell phone to communicate with others. The device may send a signal to the Target Cellular Device and thereby prompt it to send signals that include the unique identifier of the device. Law enforcement may monitor the signals broadcast by the Target Cellular Device and use that information to determine the Target Cellular Device's location, even if it is located inside a house, apartment, or other building.

28. The investigative device may interrupt cellular service of phones or other cellular devices within its immediate vicinity. Any service disruption to non-target devices will be brief and temporary, and all operations will attempt to limit the interference with such devices. In order to connect with the Target Cellular Device, the device may briefly exchange signals with all phones or other cellular devices in its vicinity. These signals may include cell phone identifiers. The device will not complete a connection with cellular devices determined not to be the Target Cellular Device, and law enforcement will limit collection of information from devices other than the Target Cellular Device. To the extent that any

information from a cellular device other than the Target Cellular Device is collected by the law enforcement device, law enforcement will delete that information, and law enforcement will make no investigative use of it absent further order of the court, other than distinguishing the Target Cellular Device from all other cellular devices.

29. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. This delay is justified because there is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the target cellular device would seriously jeopardize the ongoing investigation. Such disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). There is a reasonable necessity for the use of the techniques described. *See* 18 U.S.C. § 3103a(b)(2). As further specified in the attachment, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of

any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is a reasonable necessity for that seizure. *See* 18 U.S.C. § 3103a(b)(2).

30. I further request the following information from the service provider: all precision real-time location information, including E-911 Phase II data, GPS data, and latitude-longitude data, and real time cell site information; call detail records, including cell site location information for the past 30 days; subscriber information and extended subscriber information; handset information; and per call measurement data (PCMD) for the past 30 days.

31. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the target cellular device outside of daytime hours.

32. I further request that the Court order all documents in support of this application, including the affidavit and search warrant, be sealed until further order by the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize the investigation. I further request that the Court order

any service provider, or their representatives, not to disclose the existence of this warrant or investigation unless ordered to do so by the Court.

33. A search warrant may not be legally necessary to authorize all of the investigative techniques described. Nevertheless, I submit this warrant application out of an abundance of caution.

Respectfully submitted,

s/ Emily Munchiando
Emily Munchiando, Special Agent
Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

HON. ANDREA K. JOHNSTONE
United States Magistrate Judge

ATTACHMENT A

This warrant authorizes the use of the electronic investigative technique described in Attachment B to identify the location of the cellular device assigned phone number 269-358-0496, whose wireless provider is AT&T.

This Warrant also serves as a Pen Register order under 18 U.S.C. § 3123. The Court makes the following findings: Katelyn JONES, the daughter of Linda Jones, is the person to whom the pen register or trap and trace device is to be attached/applied and who is the subject of the criminal investigation; 269-358-0496 is the phone number to which the device is to be attached; and 18 U.S.C. § 875(c) is the offense, or one of the offenses, to which information relates; and

The attorney for the government has certified to this Court that the information likely to be obtained by the installation and use of the pen register or trap and trace device is relevant to an ongoing criminal investigation by the Federal Bureau of Investigation.

ATTACHMENT B

Particular Things to Be Seized
with a Cell Site Simulator or Wi-Fi Geolocation Device

This Warrant authorizes the officers to whom it is directed to determine the location of the target cellular device by collecting and examining:

1. radio signals emitted by the target cellular device for the purpose of communicating with cellular infrastructure, including towers that route and connect individual communications; and
2. radio signals emitted by the target cellular device in response to signals sent to it by the officers;

for a period of thirty (30) days, during all times of day and night. This includes monitoring non-content signaling and routing information, including all non-content packet switched data, through the installation and use of a pen register and trap and trace device pursuant to 18 U.S.C. § 3123 by the Federal Bureau of Investigation. Because the use of the device, a Cell Site Simulator or Wi-Fi geolocation device, may fall within the definitions of a "pen register" or a "trap and trace device," see 18 U.S.C. § 3127(3) & (4), the application and the warrant are designed to comply with the Pen Register Statute as well as Rule 41. The application therefore includes all information required for and serves as a pen register application, 18 U.S.C. § 3123(a); similarly, the warrant therefore includes

all the information required for and serves as a pen register order, 18 U.S.C. § 3123(b).

This warrant does not authorize the interception of any telephone calls, text messages, or content based internet data. The investigative device may interrupt cellular service of phones or other cellular devices within its immediate vicinity. Any service disruption to non-target devices will be brief and temporary, and all operations will attempt to limit the interference with such devices. In order to connect with the Target Cellular Device, the device may briefly exchange signals with all phones or other cellular devices in its vicinity. These signals may include cell phone identifiers. The device will not complete a connection with cellular devices determined not to be the Target Cellular Device, and law enforcement will limit collection of information from devices other than the Target Cellular Device. To the extent that any information from a cellular device other than the Target Cellular Device is collected by the law enforcement device, law enforcement will delete that information, and law enforcement will make no investigative use of it absent further order of the court, other than distinguishing the Target Cellular Device from all other cellular devices

The Court finds reasonable necessity for use of the techniques and collection of information described. *See* 18 U.S.C. § 3103a(b)(2).

This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the information described. *See* 18 U.S.C. § 3103a(b)(2).